

CLAIMS

1. Method of transmitting information with
5 verification of transmission errors, wherein a useful
information message (M) is transmitted in a determined
frame while being associated with a determined number p
of transmission error verification bits (CRC(M), S(M))
also transmitted in said determined frame,
10 wherein a determined number p1 of said p transmission
error verification bits form a seal (S(M)) obtained
from the useful information message using a determined
sealing function, where p1 is a number less than p, and
wherein the p-p1 remaining transmission error
15 verification bits form a cyclic redundancy code
(CRC(M)) calculated from the useful information
message.
2. Method according to Claim 1 wherein the p1
20 transmission error verification bits are calculated at
the MAC protocol layer, and are then delivered to a
channel coder at the physical layer.
3. Method according to any one of the preceding
25 claims, wherein the seal is obtained by truncating to
p1 the result of the sealing function which is obtained
on a number of bits greater than p1.
4. Method according to Claim 3, wherein the sealing
30 function is of Hash-MAC type with key, with a Hash
function selected from the group comprising the MD5
function, the SHA-1 function, the SHA-256 function and
sealing functions designed on the basis of a block
encryption algorithm.
- 35 5. Method according to either one of Claims 1 and 2,
wherein the result of the sealing function is obtained
directly on p1 bits.

6. Method according to Claim 5, wherein the sealing function comprises the combination of a pseudorandom generation function (GPA) and of a non-linear coding
5 function (CNL).

7. Device for transmitting information with verification of transmission errors, comprising:
means for transmitting in a determined frame a useful
10 information message (M) associated with a determined number p of transmission error verification bits (CRC(M), S(M)) also transmitted in said determined frame, and
means for obtaining a seal (S(M)) from the useful
15 information message using a determined sealing function, which seal forms a determined number p1 of said p transmission error verification bits, where p1 is a number less than p, the p-p1 remaining bits forming a cyclic redundancy code (CRC(M)) calculated
20 from the useful information message.

8. Device according to Claim 7, comprising means for calculating the p1 transmission error verification bits at the MAC protocol layer, as well as a channel coder
25 to which said p1 bits are delivered at the physical layer.

9. Device according to either one of Claims 7 and 8, comprising means for obtaining the seal by truncating
30 to p1 the result of the sealing function which is obtained on a number of bits greater than p1.

10. Device according to Claim 9, wherein the sealing function is of Hash-MAC type with key, with a Hash
35 function selected from the group comprising the MD5 function, the SHA-1 function, the SHA-256 function and sealing functions designed on the basis of a block encryption algorithm.

11. Device according to either of Claims 7 and 8, comprising means for obtaining the result of the sealing function directly on p1 bits.
- 5 12. Device according to Claim 11, wherein the sealing function comprises the combination of a pseudorandom generation function (GPA) and of a non-linear coding function (CNL).
- 10 13. Radiocommunications equipment comprising a device according to any one of Claims 7 through 12.